REMARKS/ARGUMENTS

The above identified patent application has been amended and reconsideration is hereby requested. Claims 1-47 are now in the application. Claim 42 has been amended. Claim 47 has been added. No claims have been cancelled by this amendment.

The Examiner has rejected Claims 1, 2, 4-8, 10-22, 24-38 and 40-46 under 35 U.S.C. §102(e) as allegedly being anticipated by Etzel et al. (U.S. Patent No. 6,577,734 B1), ("Etzel").

Claim 1 calls for, "a selector for coupling the first memory to the second memory <u>via the digital data input medium</u>" (emphasis added). As such, Applicants submit that Claim 1 is not anticipated by Etzel under 35 U.S.C. §102(e).

The Examiner claims, "'a digital data input medium for receiving digital data to be encrypted; a second memory' is taught by Etzel in (Fig 5, 10, and Col 2 lines 51-60)" (Office Action, pg. 2, paragraph 3). Etzel discloses in Column 2, lines 50-56 that, "Encoder 15 then supplies the compressed result to IPS 20 via path 16. Processor 25 of IPS 20 receives the compressed information from path 16 and supplies it to head-end security module 30 for encryption using a unique program encryption key that head-end security module 30 priorly generated for that purpose." While Fig. 1 does not label a path 16, it appears from the disclosure of Etzel that the path 16 lies between the encoder 15 and the processor 25.

Assuming the path 16 is equated to the "digital data input medium for receiving digital data to be encrypted" according to

Claim 1, then it must also be the medium through which the selector couples the first memory to the second memory. The Examiner contends that Etzel discloses such a selector, referencing Fig. 5 and Col. 9, lines 10-15 (Office Action, pg. 2, paragraph 3), which portions of Etzel's disclosure describe the RISC processor 2 which can control the overall operation of a security module, assumedly including the security module 30 of Fig. 1.

As such, it is Applicants' understanding that the Examiner contends that Etzel discloses the first memory and second memory called for in Claim 1 in the form of the memory 26 and the RAM contained on the security module 30, respectively. It is also Applicants' understanding that the Examiner contends that Etzel discloses the digital input medium called for in Claim 1 in the form of the path 16 between the program encoder 15 and the processor 25, and that Etzel discloses the selector called for in Claim 1 in the form of the integral component of the security module 30.

However, Applicants submit that Etzel does not disclose a selector for coupling the first memory to the second memory <u>via the digital data input medium</u>" as called for in Claim 1 because <u>the security module 30 is not in contact with the path 16</u> as shown in Fig. 1. The memory 26 and the security module 30 of Fig. 1 are not joined by the path 16, and so the RISC processor 2 of the security module 30 cannot be said to couple the memory 26 and the security module 30 via the path 16.

Therefore, because Etzel does not disclose, "a selector for coupling the first memory to the second memory via the digital

-13-

data input medium" as called for by Claim 1, Applicants submit that Claim 1 is not anticipated by Etzel under 35 U.S.C. §102(e). Claims 2-6 are dependent on Claim 1. As such, Claim 2-6 are believed allowable based upon Claim 1 and for the additional limitations contained therein, which further potentially distinguish Claims 2-6 over the art of record.

Claim 7 calls for, "transferring the selected encryption key from the first memory to a second memory over a digital data transfer medium that is also used for transferring the digital data to be encrypted". As discussed above, Etzel does not disclose a digital data transfer medium coupling a first memory and a second memory as claimed in the claims of the present application. Therefore, Etzel cannot disclose "transferring the selected encryption key from the first memory to a second memory over a digital data transfer medium that is also used for transferring the digital data to be encrypted" (emphasis added) as called for in Claim 7. Accordingly, Applicants submit that Claim 7 is not anticipated by Etzel under 35 U.S.C. §102(e). Claims 8-11 are dependent on Claim 7. As such, Claim 8-11 are believed allowable based upon Claim 7 and for the additional limitations contained therein, which further potentially distinguish Claims 2-6 over the art of record.

Claim 12 calls for inter alia, a system comprising a first input terminal, a second input terminal, and a first output terminal. Etzel on the other hand discloses in Col. 2 lines 50-60:

-14-

"Processor 25 of IPS 20 receives the compressed information
from path 16 and supplies it to head-end security module 30
for encryption using a unique program encryption key that
head-end security module 30 priorly generated for that
purpose. As such, the unique program encryption key is
known only to head-end security module 30. When head-end
security module 30 has completed encrypting such
information, it then supplies the result to processor 25."
(emphasis added)

While the security module 30 of Etzel receives and encrypts
digital data using a key, it is shown in Fig. 1 as having only
one connection to the processor 25.   As such, the security
module 30 lacks the first input terminal, second input terminal,
and first output called for in Claim 12.

Furthermore, the security module 30 does not receive a key
from an external key storage medium as called for by Claim 12,
whether during operation of the system or otherwise.   If the IPS
20 is taken as a whole to be analogous. to the system for
encrypting digital data of Claim 12, it still fails to receive a
key from an external key storage medium as called for by Claim
12.

Lastly, Claim 12 calls for "wherein the system receives the
key from an external key storage medium via the second input
terminal during operation of the system" (emphasis added).
While Claim 12 calls for a system comprising, "an encryptor…
receiving and encrypting the digital data using the key", Etzel
discloses no way in which a key may be received from an external
key storage medium during receipt and encryption of digital data

using a key without disrupting the receipt and encryption of said digital data.

For these reasons, Applicants submit that Claim 12 is not anticipated by Etzel under 35 U.S.C. §102(e). Claims 13-29 are dependent on Claim 12. As such, Claim 13-29 are believed allowable based upon Claim 12 and for the additional limitations contained therein, which further potentially distinguish Claims 2-6 over the art of record.

Claim 30 calls for "receiving a key from an external key storage medium", and "receiving the key are performed during operation of the data encryption system". As discussed above, Etzel does not disclose receiving a key from an external key storage medium, nor does it disclose receiving the key during operation of the system; both of which are as called for by Claim 30. Accordingly, Applicants submit that Claim 30 is not anticipated by Etzel under 35 U.S.C. §102(e). Claims 31-41 are dependent on Claim 30. As such, Claim 31-41 are believed allowable based upon Claim 30 and for the additional limitations contained therein, which further potentially distinguish Claims 2-6 over the art of record.

Claim 42 has been amended to call in part for, "a first decryption key, which is different than the first encryption key" (emphasis added). The Examiner claims, "'the system comprising: a digital data transmitter comprising a first key storage medium for storing a first encryption key, a second encryption key and a first decryption key' is taught by Etzel in

(Fig 1 and 5 #13, Col 3 lines 50-60 and Col 5 lines 55-60)"
(Office Action, pg. 6). While Etzel discloses a program
encryption key which may be itself encrypted, sent between
stations, decrypted, and used to decrypt a program for viewing
by a user, Etzel does not disclose a first decryption key which
is different than the first encryption key as currently called
for in amended Claim 42. According to Claim 42, it is this
first decryption key which is used to decrypt the encrypted
digital data. As such, because Etzel does not show such a first
decryption key which is different than the first encryption key,
Applicants submit that Claim 42 is not anticipated by Etzel
under 35 U.S.C. §102(e). Claims 43-46 are dependent on Claim
42. As such, Claim 43-46 are believed allowable based upon
Claim 42 and for the additional limitations contained therein,
which further potentially distinguish Claims 2-6 over the art of
record.

New Claim 47 calls for an, "encryptor having a key storage
provided as an integral component thereon" (emphasis added).
While Etzel may disclose the security module 30, it does not
disclose a key storage of an encryptor which receives a key from
an external key storage medium via the second input terminal
during operation of the system, as currently called for in New
Claim 47. Accordingly, Applicants submit that Claim 47 is not
unpatentable over the prior art currently of record.

In view of the above amendment and remarks it is submitted
that the claims are patentably distinct over the prior art and

that all the rejections to the claims have been overcome. Reconsideration of the above Application is respectfully requested.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By _____

Colin Dorrian
Reg. No. 54,658
626/795-9900

CTD/ctd
CTD PAS606340.1-*-02/3/05 7:21 PM